CLAIMS

WHAT IS CLAIMED IS:

1. A method for obscuring the identity of the source of a message while allowing the content of the message, and subsequent messages, issued from that source to be analyzed, and wherein the source is coupled to a cable television system for receiving television programming content therefrom, said method comprising the steps of:

encrypting the content of a message issued from the source to form a first message, said first message containing source identification indicia, said first message being transmitted to a remote device;

decrypting said first message into a first decrypted message upon receipt of said first message by said remote device;

substituting said source identification indicia with anonymous identification indicia that cannot be traced back to said source identification indicia; and

encrypting said first decrypted message along with said anonymous identification indicia into a second message and transmitting said second message to a location to be analyzed.

2. The method of Claim 1 wherein said step of substituting said source identification indicia with anonymous identification indicia comprises generating said anonymous identification indicia by using a character string and a portion of said source identification indicia in a mathematical hash algorithm.

3. The method of Claim 2 wherein said step of generating said anonymous identification indicia is repeated each time a subsequent message from a particular source is received such that said anonymous identification indicia is consistent for each source.

4. The method of Claim 1 wherein the cable system is operated by a cable operator entity and wherein said second message analysis is operated by a viewership analysis entity, and wherein said step of substituting said source identification

indicia with anonymous identification indicia is performed at a secure location where the viewership analysis entity cannot gain access.

5. The method of Claim 4 wherein the viewership analysis entity can gain access to said secure location only with assistance from the cable operator entity or an agent thereof.

6. The method of Claim 4 wherein the secure location comprises a computer that is password-protected and wherein the cable operator entity, or an agent thereof, does not have the password.

7. The method of Claim 1 further comprising the step of inserting cable system source data into said first decrypted message.

8. The method of Claim 7 wherein said source data comprises cable system network segment data.

9. The method of Claim 7 wherein said source data comprises cluster code data.

10. The method of Claim 1 wherein said source is a set top box.

11. The method of Claim 1 wherein said source is a cell phone.

12. The method of Claim 1 wherein said source is a personal digital assistant.

13. A system for obscuring the identity of the source of a message while allowing the content of the message, and subsequent messages, issued from that source to be analyzed, wherein the source is coupled to a cable television system for receiving television programming content therefrom, and wherein the source encrypts the message content while embedding source identifier indicia in the encrypted message, said system comprising a server, said server comprising:

means for decrypting the encrypted message into a first decrypted message;

means for generating anonymous identification indicia and for substituting the source identifier indicia with said anonymous identification indicia to

form a first decrypted message having said anonymous identification indicia embedded therein, said anonymous identification indicia preventing said first decrypted message from being traced back to said source identifier indicia;

means for encrypting said first decrypted message having said anonymous identification indicia embedded therein to form a second encrypted message having said anonymous identification indicia embedded therein; and

wherein said server transmits said second encrypted message having said anonymous identification indicia to message content analysis means.

14. The system of Claim 13 wherein said means for generating anonymous identification indicia comprises a computer-readable medium having computer-executable instructions for using a character string and a portion of said source identification indicia in a mathematical hash algorithm to generate said anonymous identification indicia.

15. The system of Claim 14 wherein said means for generating anonymous identification indicia repeats the use of said mathematical hash algorithm each time a subsequent message from a particular source is received such that said anonymous identification indicia is consistent for each source.

16. The system of Claim 15 wherein said source is a set top box.

17. The system of Claim 15 wherein the source comprises a memory chip that permits said source to receive the television programming content and wherein said source is a cell phone.

18. The system of Claim 15 wherein the source comprises a memory chip that permits said source to receive the television programming content and wherein said source is a personal digital assistant.

19. The system of Claim 13 wherein the cable system is operated by a cable operator entity and wherein said message content processing is managed by a viewership analysis entity,

said server being positioned at a secure location where the viewership analysis entity cannot gain access.

20. The system of Claim 19 wherein said viewership analysis entity can gain access to said secure location only with assistance from the cable operator entity or agent thereof.

21. The system of Claim 19 wherein said means for generating anonymous identification indicia comprises a computer that is password-protected and wherein the cable operator entity does not have the password.

22. The system of Claim 15 further comprising means for inserting cable system source data into said first decrypted message.

23. The method of Claim 22 wherein said source data comprises cable system network segment data.

24. The method of Claim 22 wherein said source data comprises cluster code data.